COMPUTER ACCESS CONTROLS FOR COMPUTER SERVICES

COPYRIGHT NOTICE

[0001] A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or patent disclosure as it appears in the U.S. Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

TECHNICAL FIELD

[0002] The present disclosure relates generally to personal computers and, more particularly, to systems and methods for controlling computer access.

BACKGROUND

[0003] With the growth of computers, many households have computers that are utilized by users of various ages. However, the primary user of a computer may want to limit the services or applications performed by a computer for him or herself or other users. For example, the primary user may desire to limit the displaying of unsolicited communications that are received over the Internet. Also, the primary user may want to limit the computing resources that are available to a child, for example. Currently, software applications exist, which attempt to limit the computing resources or services performed by a computer. Such applications, however, still may not be adequate to effectively limit computing resources in a manner that is preferable to the primary user of the computer.

[0004] Thus, a heretofore unaddressed need exists in the industry to address the aforementioned deficiencies and inadequacies.

SUMMARY

[0005] The present disclosure provides systems and methods for controlling access to computing services. Some embodiments provide access control mechanisms for controlling access to computer applications and services based on settings within a

user's configuration profile. The configuration profile of user of a general-purpose computer is specified by the primary user of the general-purpose computer. In this manner, the primary user of the general-purpose computer may control and regulate the type of access that others users of the general-purpose computer have to local computer applications and other computer services.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Many aspects of the disclosure can be better understood with reference to the following drawings. The components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views.

[0007] FIG. 1 is a block diagram of a system for controlling access to computer services for embodiments of the present disclosure.

[0008] FIG. 2 is a flowchart describing one embodiment of a process for controlling access to computer applications for the system of FIG. 1.

[0009] FIG. 3 is a flowchart describing one embodiment of a process for controlling access to a computer application for the system of FIG. 1.

[0010] FIG. 4 is a flowchart describing one embodiment of a process for controlling access to a Windows Messenger Service application for the system of FIG. 1.

[0011] FIG. 5 is a flowchart describing one embodiment of a process for controlling access to a particular service performed by a computer application for the system of FIG. 1.

[0012] FIG. 6 is a flowchart describing one embodiment of a process for determining if a user is authorized to access a particular Internet address for the system of FIG. 1.

[0013] FIG. 7 is a flowchart describing one embodiment of a process for providing a user report for the system of FIG. 1.

[0014] FIG. 8 is a flowchart describing one embodiment of a process for categorizing communication services and applications for the system of FIG. 1.

[0015] FIG. 9 is a flowchart describing one embodiment of a process for synchronizing the contents of user-related information for the system of FIG. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Reference is now made in detail to the description of the embodiments as illustrated in the drawings. While several embodiments are described in connection with these drawings, there is no intent to limit the invention to the embodiment or embodiments disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0017] The present disclosure provides systems and methods for controlling access to computing services. FIG. 1 is a block diagram of one embodiment of the system 100 for controlling access to computing services. As shown in FIG. 1, the access control system 100 comprises general-purpose computers 102, 104, 106 that are coupled to a server 110 over a network such as the Internet 120. Typically, the communication network 120 provides access to Internet services such as email, FTP, WWW, IRC, *etc.* and newsgroups, such as Usenet. The server 110 is coupled to a database 115 that stores user configuration profiles of various users.

[0018] In the operating environment shown in FIG. 1, a user of a general-purpose computer 106 attempts to access applications on the computer 106 and services over the network 120. As shown in FIG. 1, the general purpose computer 106 includes a processor 152, a network interface 160, memory 154, a local storage device 158, and a bus 156 that permits communication between the various components. While not explicitly shown, it should be appreciated that the other computers 102, 104 may also include similar components that facilitate computation or execution of applications on the computers 102, 104. In some embodiments, the local storage device 158 may be a hard drive configured to electronically store data. The local storage device 158 may also store computer programs that execute on the computer 106. In this sense, the processor 152 is configured to access any program that is stored on the local storage device 158, and execute the program with the assistance of the memory 154.

[0019] The network interface 160 is configured to provide an interface between the general-purpose computer 106 and the network 120. Thus, the network interface 160 provides the interface for the computer 106 to receive any data that may be entering from the network 120 and, also, to transmit any data from the computer 106 to the network 120. Specifically, in some embodiments, the network interface 160 is configured to permit communication between each of the computers 102, 104, 106 and the server 110 and, additionally, to permit communication between the computers 102, 104, 106 themselves. In this regard, the network interface 160 may be a modem,

a network card, or any other interface that communicatively couples each of the computers 102, 104, 106 to the network. Since various network interfaces are known in the art, further discussion of these components is omitted here.

[0020] In the embodiment of FIG. 1, an access control unit 155 is shown as being loaded into memory 154 for launching at the general-purpose computer 106, thereby permitting a primary user or administrator to control which applications may be accessed by other users of the computer 106. Further, the primary user may control which communications from the network 140 are accessible or displayed to users of the general-purpose computer.

I. Architecture

[0021] The access control unit 155 of the present embodiment can be implemented in software, firmware, hardware, or a combination thereof. Preferably, the access control unit 155 is implemented in software, as an executable program, and is executed by a special or general-purpose digital computer 106, such as a personal computer, workstation, minicomputer, or mainframe computer.

[0022] The memory 154 can include any one or combination of volatile memory elements (*e.g.*, random access memory (RAM, such as DRAM, SRAM, *etc.*)) and nonvolatile memory elements (*e.g.*, ROM, hard drive, tape, CDROM, *etc.*). Moreover, the memory 154 may incorporate electronic, magnetic, optical, and/or other types of storage media. Note that the memory 154 can have a distributed architecture, where various components are situated remote from one another, but can be accessed by the processor 152.

[0023] The software in memory 154 may include one or more separate programs, each of which comprises an ordered listing of executable instructions for implementing logical functions. In the example of FIG. 1, the software in the memory 154 includes the access control unit 155, an Internet browser application 180, and an operating system (O/S) 170. The operating system 156 essentially controls the execution of other computer programs, and provides scheduling, input-output control, file and data management, memory management, and communication control and related services.

[0024] The access control unit 155 may be a source program, executable program (object code), script, or any other entity comprising a set of instructions to be performed. If the access control unit 155 is a source program, then the program needs

to be translated via a compiler, assembler, interpreter, or the like, which may or may not be included within the memory 154, so as to operate properly in connection with the O/S 170. Furthermore, the access control unit 155 can be written as (a) an object oriented programming language, which has classes of data and methods, or (b) a procedure programming language, which has routines, subroutines, and/or functions, for example but not limited to, C, C+ +, Pascal, Basic, Fortran, Cobol, Perl, Java, and Ada.

[0025] The I/O devices 190 may include input devices, for example but not limited to, a keyboard, mouse, scanner, digital camera, multi-function device, digital sender, microphone, *etc.* Furthermore, the I/O devices 190 may also include output devices, for example but not limited to, a printer, display, *etc.* Finally, the I/O devices 190 may further include devices that communicate both inputs and outputs, for instance but not limited to, a modulator/demodulator (modem; for accessing another device, system, or network), a radio frequency (RF) or other transceiver, a telephonic interface, a bridge, a router, *etc.*

[0026] The software in the memory 154 may further include a basic input output system (BIOS) (omitted for simplicity). The BIOS is a set of essential software routines that initialize and test hardware at startup, start the O/S 170, and support the transfer of data among the hardware devices. The BIOS is stored in ROM so that the BIOS can be executed when the computer 106 is activated.

[0027] When the computer 106 is in operation, the processor 152 is configured to execute software stored within the memory 154, to communicate data to and from the memory 154, and to generally control operations of the computer 106 pursuant to the software. The access control unit 155, Internet browser 180, and the O/S 170, in whole or in part, but typically the latter, are read by the processor 152, perhaps buffered within the processor 152, and then executed.

[0028] When the access control unit 155 is implemented in software, as is shown in FIG. 1, it should be noted that the access control unit 155 can be stored on any computer readable medium for use by or in connection with any computer related system or method. In the context of this document, a computer readable medium is an electronic, magnetic, optical, or other physical device or means that can contain or store a computer program for use by or in connection with a computer related system or method. The access control unit 155 can be embodied in any computer-readable

medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions.

[0029] In the context of this document, a "computer-readable medium" can be any means that can store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer readable medium can be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples (a nonexhaustive list) of the computer-readable medium would include the following: an electrical connection (electronic) having one or more wires, a portable computer diskette (magnetic), a random access memory (RAM) (electronic), a read-only memory (ROM) (electronic), an erasable programmable read-only memory (EPROM, EEPROM, or Flash memory) (electronic), an optical fiber (optical), and a portable compact disc read-only memory (CDROM) (optical). Note that the computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance optical scanning of the paper or other medium, then compiled, interpreted or otherwise processed in a suitable manner if necessary, and then stored in a computer memory.

[0030] In an alternative embodiment, where the access control unit 155 is implemented in hardware, the access control unit 155 can be implemented with any or a combination of the following technologies, which are each well known in the art: a discrete logic circuit(s) having logic gates for implementing logic functions upon data signals, an application specific integrated circuit (ASIC) having appropriate combinational logic gates, a programmable gate array(s) (PGA), a field programmable gate array (FPGA), *etc.*

II. Operation

[0031] The flowcharts of FIGs. 2-9 show the functionality of a representative implementation of the system 100 for controlling access to computing services of the present embodiment. It should also be noted that in some alternative implementations the functions noted in the various blocks may occur out of the order depicted in the

flowcharts of FIGs. 2-9. For example, two blocks shown in succession in FIGs. 2-9 may, in fact, be executed substantially concurrently. Alternatively, the blocks may sometimes be executed in the reverse order depending upon the functionality involved.

[0032] As depicted in FIG. 2, the functionality of a representative embodiment of the system for controlling access to computing services 100 or method 200 may be construed as beginning at block 210. In block 210, a primary user (or administrator, such as a parent) of a general purpose computer 106 specifies that user-access to a particular computer application or program (stored locally on the computer 106) is to be controlled and regulated by the access control unit 155. Accordingly, the primary user creates a configuration profile for each user of the general-purpose computer 106 that specifies the type of access each user is to have to the particular application. For each user, the configuration file contains a username and password for the user. For example, a parent may act as an administrator and create configuration profiles for each child of the parent that utilizes the computer 106. The parent, therefore, establishes a master configuration profile or account for him or herself and configuration profiles for each child of the parent ("sub-accounts" of the master account). For example, when the primary user sets up the access control unit 155 on the general-purpose computer 106, the primary user typically accesses the server 110 to define a configuration profile for each child or user of a sub-account. Each configuration profile is stored in the database 115 on the network 120 and is accessible from the server 110 using the World Wide Web (WWW). A copy of the configuration profile for each user is also stored on the general-purpose computer 106.

[0033] Accordingly, the primary user (e.g., parent) may access the configuration profile of a user (e.g., a child) by facilitating communication between any general purpose computer with an Internet browser 180 and the server 110. Upon certain computer events, the configuration profiles on the general-purpose computer 106 and the database 110 are "synchronized" so that the copies of the configuration profiles stored in the general-purpose computer 106 are the most current versions of the configuration profile stored in the database 115 at the time of synchronization. For example, the access control unit 155 attempts to retrieve the latest configuration profiles for each user when any user logs into the access control unit 155, when a user

logs off of the access control unit 155, when the Internet browser application 180 is launched, and when the computer 106 is turned on.

[0034] Within the configuration profile of a user, the primary user may specify (220) a particular computer application that the user is to be denied access to. Accordingly, when a user attempts to access any computer application on the general purpose computer 106, the access control unit 155 intercepts (225) the command to launch the application and checks (230) to see if the user is attempting to access the particular computer application whose access is being regulated by the access control unit 155. If the particular computer application that the user is attempting to access is being regulated by the access control unit 155 (for any user), the access control unit 155 determines (240) the identity of the current user that is attempting to access the computer application. Otherwise if access to the particular application is not being regulated, the access control unit 155 processes (245) the command to launch the computer application.

[0035] To determine the identity of the current user, the access control unit 155 prompts the user to enter his or her username and password. Upon receiving the username and password, the access control unit 155 identifies the user and checks (250) the copy of the user's configuration profile that is stored in the general purpose computer 106 to determine whether the user is allowed to access the particular computer application. If the user is authorized, then the access control unit 155 processes (260) the command to launch the computer application. If the user is not authorized, then the command to launch the computer application is not processed (270) and the user is denied or prohibited access to the computer application. Note, the primary user may prevent access to multiple computer programs and applications for each user (of a sub-account) and may impose different access restrictions for different users.

[0036] In some embodiments, the operating system 170 is a MICROSOFT WINDOWS-based operating system (98, ME, XP, 2000, NT, *etc.*). Note, WINDOWS is essentially a message driven operating system in the sense that, the majority of actions that take place are responses to messages sent to the main window procedure of an application. One approach, among others, for intercepting messages in the windows environment involves hook mechanisms that can monitor and intercept messages before the WINDOWS O/S 170 has decided which application to direct the

message to. Accordingly, the access control unit 155 may intercept any messages from an application that attempts to open a window and determine whether the application is prohibited before processing the message further. Note, other mechanisms may be used to intercept commands to launch applications within the windows operating system and other operating systems and are contemplated by the present disclosure.

[0037] For example, FIG. 3 illustrates one implementation of the method 200 for restricting access to a computer application, such as an Internet browser application 180. First, an administrator (e.g., primary user of the general computer 106) assigns (310) access rights to the Internet browser application 180 for other users of the general-purpose computer 180. Accordingly, the administrator may allow one user to access the Internet browser application 180 and deny access to another user. For example, the administrator may specify in the configuration profile of a user that access to the Internet browser application is to be prohibited for that user. Next, the access control unit 155 monitors (320) messages from applications on the general-purpose computer 106 that attempt to open a new window to launch the application. To illustrate, a user may use a mouse to "double click" on an Internet browser icon on a windows desktop to attempt to "open" the Internet browser application 180. The Internet browser application 180 generates a request to open a new window to activate an instance of an Internet browser.

[0038] Since most Internet browsers are windows-based, they provide application-specific mechanisms (*e.g.*, hook functions) for monitoring whether the Internet browser is attempting to launch a new window for a web page in a similar manner as the Windows operating system. For example, an INTERNET EXPLORER helper object can install hooks to monitor and control messages and actions of the INTERNET EXPLORER browser.

[0039] Accordingly, upon detection of a message or request to open a new window from an application to the O/S 170, the access control unit intercepts (330) the message and determines (340) if the message is from an application that is prohibited or regulated for any of the users associated with the general-purpose computer. If the message is from a particular application whose access is limited in at least one user's configuration profile, the identity of the current user is ascertained (350) to determine if the current user is authorized to access the particular application. If the message is

from a particular application whose access is not limited for any user of the general-purpose computer 106, the message to open a new window is processed (360) and forwarded passed to the O/S 170 so that the application may be launched 180.

[0040] To ascertain the identity of the current user (who is not already known), the access control unit 155 may prompt the user to identify him or herself by requesting the username and password for the user. Once the current user has logged in with the access control unit 155, the user does not need to identify him or herself unless the current user logs off, or if the computer is restarted. After the user identifies him or herself, the access control unit 155 checks (370) with the user's configuration profile that is stored locally on the general purpose computer 106 to determine if the user is authorized to access the particular application, such as the Internet browser 180. If the user is authorized, then the access control unit 155 processes (380) the message for opening the new window in order to launch the particular application, such as the Internet browser 180. Note, in some embodiments, upon launching the Internet browser 180, the access control unit 155 retrieves the latest configuration profile for the user.

[0041] FIG. 4 illustrates another implementation of the method 200 with regard to a Windows Messenger Service which is part of the MICROSOFT WINDOWS operating system (98, ME, XP, 2000, NT, *etc.*). Via Windows Messenger Service, unsolicited messages are often received on a user's computer 106 that is connected to the Internet 120. Thus, the access control unit 155 may be configured (410) to prohibit access to messages from the Windows Messenger Service. For example, the access control unit 155 may block access to the Windows Messenger Service as a default operation for all users of the general-purpose computer 106. Note, in other embodiments, a primary user of general-purpose computer 106 may specify which users are able to access to the Windows Messenger Service.

[0042] Accordingly, once the Windows Messenger Service sends a message for opening a new window to display a Windows Messenger Service message on the general-purpose computer 106 (that might have been received from the Internet), the access control unit 155 intercepts (420) the message. For this example described in FIG. 4, the access control unit 155 prevents access to the Windows Messenger Service for all users of the general-purpose computer. Therefore, the access control unit 155

prevents (430) the message for opening a new window (for displaying the Windows Messenger Service message) from being processed.

[0043] While the primary user may authorize a user to activate or launch a particular computer application, some embodiments of the access control unit 155 can also regulate access to certain features or services of particular computer applications for particular users. For example, the primary user may prohibit an instant messaging application from displaying messages directed to a particular user from a sender who is not authorized by the primary user.

[0044] For example, FIG. 5 illustrates one implementation of a method 500 for restricting access to a particular service performed by a computer application, such as an Internet browser application 180. First, an administrator (e.g., primary user of the general computer 106) assigns (510) access rights to for a particular service performed by a particular computer application, such as an Internet browser application 180. The access rights are assigned for other users of the general-purpose computer 180. Accordingly, the administrator may allow one user to access some services or features of the Internet browser application 180 that are denied to other users. For example, the administrator may specify in the configuration profile of a user that access to a particular web page address (Internet address) from the Internet browser application is to be prohibited for that user. Further, the primary user may specify instant messaging addresses that a particular user is allowed to receive instant messages from. In addition, the primary user may specify which local applications are to be blocked, such as instant messaging applications, email applications, newsgroup applications, file transfer applications, games, banking applications, etc, as previously described with regard to FIG. 2.

[0045] Next, the access control unit 155 monitors (520) messages from the particular application (e.g., Internet browser application 180) that pertain to the particular service that is being regulated. For example, if the particular service is a message request for a certain web page, the access control unit 155 monitors all requests that generated by the Internet browser application 155 for retrieving a web page.

[0046] Accordingly, upon detection of a message or request related to the particular service being regulated (e.g., request to rctricve a web page), the access control unit intercepts (530) the message and determines (540) if the message is for a service that

has been specifically prohibited for the current user of the particular application (who has previously logged into the access control unit 155).

[0047] The access control unit 155 checks (550) with the current user's configuration profile that is stored locally on the general purpose computer 106 to determine if the current user is authorized to access the particular application service, such as access to a particular web page. If the user is authorized to access the particular service, then the access control unit 155 processes (560) the message relating to the particular service. However, if the user is not authorized to access the particular service, then the access control unit 155 does not process (570) the message relating to the particular service.

For example, when the current user initiates a request for a web page (at an Internet address) from the Internet browser 180, the access control unit 155 intercepts (540) the command to retrieve the web page at the specified internet address (e.g., URL). Then, the access control unit 155 checks to determine if access to the Internet address should be prohibited.

[0048] In some embodiments, the primary user may generally block categories of communications from the Internet. For example, a primary user may prevent another user from accessing web pages that have been categorized as "Violent," "Pornographic," etc. by the access control unit 155. Therefore, the access control unit 155 determines (550) whether a particular website fits a certain categorization and if a particular user has been prohibited from accessing communications of that categorization. If the particular user is prohibited from accessing communications of that particular categorization, then access control unit 155 blocks (560) access to the web page by not processing the command from the Internet browser to retrieve the web page. Otherwise, the command to request the web page is processed (570).

[0049] To facilitate the operation of checking (550) for authorized categories of web pages, the database 115 on the network maintains a list of websites that are accessible via the Internet and categories or ratings for each website. This list is continually updated. In some embodiments, for example, a ratings service provided by a third party may provide an XML feed to the database 115 for providing current ratings or content categories of websites on the Internet 120. Further, categories employed by the access control unit 155 may be different from the categories provided by the third party rating service. However, the categories provided by the third party rating service

may be mapped to the categories employed by the access control unit 155. Note, if a requested website by a user does not fall into a category employed by the access control unit 155, the primary user can still block access to the website by listing the website in the user's "blacklist" in the user's configuration profile. Particularly, the primary user may specify particular websites that are to be prohibited by listing specific domain names on a blacklist for each user. Correspondingly, the primary user may also specify particular websites that are allowed to be accessed by a particular user by listing the specific domain name for the particular website on a "whitelist" that is contained in the user's configuration profile.

[0050] Therefore, FIG. 6 shows a process for determining if a requested Internet address is authorized by the primary user, as implemented in some embodiments. First, the access control unit 155 checks (610) to see if the requested Internet address (URL) is authorized by checking to see if the Internet address is contained in particular user's whitelist (in the user's configuration profile). If the requested Internet address is contained in the whitelist, then access to the requested Internet access is granted (620). If the requested Internet address is not contained in the whitelist, the user's blacklist (in the user's configuration profile) is checked (630) to see if the requested Internet address is specifically prohibited. If the requested Internet address is on the user's blacklist, then access to the web page located at the Internet address is not granted (640). However, if the requested Internet address is not on the user's blacklist, the access control unit 155 sends (650) a look up request to the server 110 for the requested Internet address. The server 110 responds (660) by returning the rating or categorization of the requested Internet address. Then, the access control unit 155 checks (670) to see if the user is authorized to access communication of that categorization based on the user's configuration profile. If the user is authorized for the categorization returned from the server 110, the command to retrieve the requested web page is processed (680).

[0051] If the user is not authorized, a web page is retrieved (690) from the server informing the user that the user is not authorized to view the requested web page. Further, in some embodiments, the web page provides (695) a mechanism for allowing the user to make a request to the primary user for authorization to access the prohibited web site.

[0052] Accordingly, the primary user may access a variety of web pages from the server that allow the primary user to configure and amend configuration profiles of users that were registered by the primary user. Further, the primary user may view the applications and services that a user of a sub-account has requested access to. Typically, this information is provided via a web page from the server. On the same web page, the primary user may grant or deny access to the requested application or service (e.g., access to a web page). Upon response to a request, configuration profiles of the user is updated. Accordingly, updating of the copy of the configuration profile at the computer 106 may occur at user login/logout, open of the Internet browser, or startup of the computer 106. Note, in other embodiments, requests may be sent via email.

[0053] From the web pages provided by the server 115, the primary user also may view online reports on which applications and communication services (that are being regulated by the access control unit) have been accessed by each user via the World Wide Web. In this way, the primary user may monitor and configure the access control unit 155 remotely from other computers besides the general-purpose computer 106 that the access control unit 155 resides on. Reports are provided for each user of a sub-account. Each report contains a detailed history of a user's use of services and applications that are regulated by the access control unit 155. In some embodiments, the primary user can view the last 24 hours of activity, the last 7 days of activity, and the last 30 days of activity with regard to these services and applications. Further, from these web pages provided by the server 110, the primary user can add services or applications to a user's whitelist and/or blacklist. Since these online user reports are provided via web pages, the primary user can access the reports from any computer that has access to the World Wide Web. In alternative embodiments of the invention, user reports may be provide by another manner such as email.

[0054] FIG. 7 illustrates one implementation of a method 700 for providing user reports to the administrator or primary user of the general-purpose computer 106. First, the administrator specifies (710) which applications and application services that the access control unit should 155 monitor and record for a particular user. Typically, these are the applications and application services that are specified in the configuration profile of the user. Correspondingly for each user of the general-purpose computer, the access control unit records (720) the time of day that the

particular applications/services are accessed and the duration of access for applications/services specified in the configuration profile for each user. The information containing the user-access times are transferred to a network server 110 and stored (730) in the database 115 upon the occurrence of particular computer events as previously described with reference to FIG. 2 (e.g, log in, log out, start-up, activating an instance of an Internet browser, user command, etc.).

[0055] As previously described, the server (110) provides (740) the access times (in the form of a report) for a particular user to the administrator over the network 120 via the World Wide Web. From the web pages provided by the server 110, the primary user also may view reports on which applications and application services (that are being regulated by the access control unit) have been accessed by each user or have been denied access by each user via the World Wide Web. Each report contains a detailed history of a user's use of services and applications that are regulated by the access control unit 155. As stated above, the primary user can view the last 24 hours of activity, the last 7 days of activity, and the last 30 days of activity with regard to these services and applications, in some embodiments. Further, from these web pages provided by the server 110, the primary user can add (740) services or applications to a particular user's whitelist and/or blacklist.

[0056] FIG. 8 illustrates another implementation of a method 800 with regard to the bundling of Internet services and computer applications under single categories. In some embodiments, in addition to categorizing web pages within certain categories, local computer applications may also be included (810) within the same categories. For example, an "Email" category may include web-based email services along with email applications that are stored on the general-purpose computer. Further, a "Message Board" category may include specific web-based message boards and message board type applications, such as newsgroup readers.

[0057] In this way, the primary user may comprehensively prohibit (820) a particular user from accessing applications or services of the "Email" category, for example, as defined within the configuration profile of the user. Typically, the access control unit 155 provides predefined web sites and computer applications within each predefined category. However, the user can also specify additional applications and web sites. The access control unit 155 maintains a list of applications and websites that fit into each category. To update this list, a user may instruct the access control unit 155 to

check for updates from the server 110 and download a new list from the server 110 if available.

[0058] Therefore, the access control unit 155 intercepts (830) any command (or message) from any application to launch a new window. The access control unit 155 determines (840) whether the access is being regulated by the access control unit 155. If access to the application that generated the command to launch the new window is not being regulated, the command to open the new window is processed (850). If the application/service is being regulated however, the access control unit determines (860) if the application is on the user's whitelist. If the application is on the user's whitelist, the application is launched (870). If the application is not on the user's whitelist, the application is checked (875) to see if it is on the user's blacklist. Accordingly, if the application is on the user's blacklist, the command to launch a new window is not processed (880). If the application is not on the user's blacklist, the access control unit 155 determines (885) the type of category that the application has been rated at, if any. If the application belongs to a category that has been prohibited by the primary user, the command to open the new window is not processed (890).

[0059] When the user has been prohibited from accessing a computer application, a display window is shown indicating that the user is not authorized to access the particular application. As previously discussed, the user may also be prohibited from viewing web pages that are of a certain category of application/service that has been disallowed by the primary user. Alternatively, if the user is authorized to access the category of application, then the user is granted (895) access to the application by processing the command to open the new window. Note, to identify particular applications on the general-purpose computer 106, identification information may be extracted from the executable file for that particular application.

[0060] As a security feature, in some embodiments, the access control unit 155 is configured to allow users of the general-purpose computer 106 to have access to only a designated Internet browser so that communications from non-designated Internet browsers are intercepted and not processed. In this way, users cannot attempt to bypass the access control measures by installing and running other Internet browsers. In other embodiments, software applications may be prohibited from being utilized by a user of a general-purpose computer. In this way, a provider of computer application

software can ensure that specific models of software are used in collaboration with the computer application software.

[0061] In addition to designating which category types of applications and services may be accessed by a user, the primary user, via the access control unit 155, in some embodiments, can specify access times that a user may specify a particular category of services/applications (e.g., email), a particular service (e.g., web access to a website), or a particular application (e.g., a computer game). Times may be specified by duration, such as two hours of access, or specific times of day, such as 5 p.m. to 8 p.m. Access times can be specified per user of a sub-account and per services, applications, and categories. The access times are stored in a user's configuration profile and may be accessed from the server 110 via the World Wide Web, as previously mentioned. Note, a clock maintained at the server 110 is used for timing purposes instead of a local clock on the general-purpose computer 106. In this way, a user of the general-purpose computer 106 cannot manipulate local clock settings to avoid time restrictions initiated by the primary user.

[0062] FIG. 9 illustrates one implementation of a method 900 for synchronizing or coordinating the contents of user-related information stored on the database 115 and the general-purpose computer 106. As previously described, information contained in configuration profiles stored on either the database 115 or the general-purpose may be modified by the access control unit 155. For example, an administrator may make changes to a user's configuration profile stored on the database 115 via the World Wide Web. Also, the application control unit 115 also records the times and duration that a user accesses certain applications and/or application services. Accordingly, such user-related information is periodically synchronized so that the information contained within the database matches the information contained in the general-purpose computer.

[0063] First, upon start-up of the general-purpose computer, the access control unit 155 determines (910) if the general-purpose computer is connected to the network 120 (e.g., the Internet). If the general-purpose computer is connected to the Internet, the access control unit synchronizes (920) the information contained within the general-purpose computer 106 with the database 115. If the general-purpose computer is not connected to the Internet, then the access control unit does not attempt the synchronization procedure.

[0064] The synchronization process may be generally described as follows. Since the configuration profiles stored in the database 115 are the most current versions, the access control unit 115 downloads the configuration profiles for each user from the database 115 so that the configuration profiles at the database 115 and the general-purpose computer 106 match. Correspondingly, the most recent access timing information recorded by the access control unit 155 is sent to the database 115 (via the server 110) for each user.

[0065] Next, upon a user logging into the access control unit 155, the access control unit attempts to perform (920) the synchronization procedure (as previously described). Likewise, if the access control unit cannot make a connection with the network 120 and the database 115, the synchronization operation is not performed. Further, upon a user logging off the access control unit 155, the access control unit also attempts to perform (930) the synchronization procedure.

[0066] The activation of an instance of an Internet browser may also cause the access control unit to attempt to perform (940) the synchronization procedure. Plus, a current user of the general-purpose computer may manually enter a command for the synchronization procedure to be attempted to be performed (950), as previously described.

[0067] Typically, the access control unit 155 may be downloaded by a user as a separate software module. However, in some embodiments, the access control unit 155 may be integrated into other software applications such as an Internet browser 180 or other access control mechanisms, such as pop-up window blocking software.

[0068] Any process descriptions or blocks in flow charts should be understood as representing steps in the process, and alternate implementations are included within the scope of the embodiments of the present disclosure in which steps may be executed out of order from that shown or discussed, including substantially concurrently or in reverse order, depending on the functionality involved, as would be understood by those reasonably skilled in the art of the present disclosure.

[0069] It should be emphasized that the above-described embodiments are merely possible examples of implementations, merely set forth for a clear understanding of the principles of the disclosure. For example, sample embodiments, among others, and other related materials are included in Appendices 1-2. Many variations and modifications may be made to the above-described embodiment(s) without departing

substantially from the spirit and principles of the invention. All such modifications and variations are intended to be included herein within the scope of this disclosure.

APPENDIX 1

BellSouth Parental Controls

Training Guide/Product Overview

Table of Contents

- Customer Perspective
- Success Criteria

2. Product Technology
    - What are BellSouth Parental Controls?
    - Why should I have Parental Controls?
    - How does it work?
    - System Preferences

3. Installing the Client
    - User Authentication
        1. Figure 1 Download Flow
        2. Figure 2 Download Screens
        3. Figure 3 Set-Up
4. Error Messages
    - Non-BellSouth IP Error Page
    - Non-IE Browser Error Page
    - MacIntosh Error page

5. Blocked Sites messages to children
    - Message when Category is blocked
    - Message when Access to application is denied
    - Message when Child has gone over time set.
    - Area where child makes request to parents

6. System Tray Operation
    - System tray menu
    - Parental Controls Manager
    - Enable/Disable

7. Frequently Asked Questions

Section I. Marketing Overview

1: Product Description

a) Product definition and value proposition

- BellSouth Internet Service will offer a FREE and easy-to-use Parental Control product that gives parents the ability to restrict their family's access to online content and activities. Parental Controls will help parents provide their children with a safe, fun and enriching online experience by enabling them to define and control access to Websites, email, IM, chat room, newsgroup and file sharing activity.

- VISION: Parental Controls will compliment BellSouth's suite of easy-to-use and convenient Internet protection products (ie: Anti-SPAM, Anti-Virus, Pop-up Blocker & Parental Controls) that will help customers enjoy a safe and secure computing environment by offering them protection from many of the hazards of being online.

- BIS Parental Controls will limit a computer's Internet access to the following 2 browser options …. And the Parental Control software will block all other browsers from working.
  - Software plug-in for Internet Explorer 4.0+
    - 93% of BellSouth Internet Service customers use Internet Explorer. It's estimated that over 90% of IE users use version 4.0+.
  - Customized BellSouth browser
    - The Parental Control software plug-in comes with the BellSouth browser

b) **Product features for this launch**

- There are 3 basic categories of Parental Control restriction. Each category has pre-defined default limitations. During set-up, parents will be asked to select a category for each family member to help determine their general level of access …. and parents can adjust the default category restrictions as desired. Parental Controls users can define up to 5 family member profiles.
  - KID: Extremely restrictive. Blocks content inappropriate for children 12 and under. Includes blocking of email, IM, NewsGroups, chat rooms and file sharing.
  - TEEN: Limited restrictions. Provides more freedom, but does not provide full access to the Internet. Blocks content inappropriate for children aged 13-18.
  - ADULT: Full access to the Internet with no blocking of sites, activities, etc.

- Parents can define specific Internet restrictions.
  - General Internet usage guidelines (ie: "time of day", "day of the week", and "maximum amount of time online" for each family member)
  - Restriction for visiting and blocking specific Internet websites and/or types of websites
  - Allow or Ban access to email, IM, NewsGroups, chat and file sharing. Note: Parents either "allow or block" these activities. There will be no "limiting" capability at launch.

- Children to easily send their parents a request to access a blocked website or activity.

- BIS Parental Controls can be used on multiple household computers. Parent may download and configure the Parental Control software each PC. Then, family profiles can easily be set-up once via the Portal .... and parents can return to the Portal to update their family profiles anytime.

- Parents can receive a weekly Internet activity report. Reports for each sub account include:
  - Sites visited (parents will be able to view and block)
  - Sites attempted but blocked (parents will be able to click to unblock)
  - Time spent online by activity (Websurfing, email, IM, chat room, newsgroup and file sharing)

- Parents are notified if a family member attempts to modify their Parental Control profile, load new browsers on the computer, or otherwise try to circumvent or remove their defined restrictions.

c) The following desired product features may be included in another embodiment

- Ability to block websites based on "keywords"
- "Restricted Access" to email, IM, chat room, newsgroup and file sharing activity
  - Define who can / can't send emails and IMs to your child
  - Filter emails with undesirable text and SPAM emails to the parents (and not the kid's) email account. Should put these emails in a new "Parental Controls folder".
  - Define what specific chat room, NewsGroup and file sharing activity your will allow.
  - Block, filter, record, and monitors IM, chat room sessions and NewsGroup postings
- Protect "confidential information". Gives parents the option to block outgoing personal information like credit card numbers, address, phone number, school, etc.

II. Market Situation

a) Research / Market trends / Customer needs analysis

- Online safety for young Internet users is a growing concern
  - 45% of US children use the Internet
  - 97% of children ages 12-18 use the Internet
  - 18% of young Internet users received an unwanted sexual solicitation in the past year.
    - 89% of solicitations were made in either chat rooms or instant messages.

- 70% of those unwanted solicitations happened when the youth was using a computer at home

- Parental Controls protection is very important to Internet users.
  - 38% of BIS customers have children under 18 years old living in their household.
  - 73% of these youngsters use the their parents FastAccess DSL service (27% of the overall base have kids who use BIS)
    30% of users report that it's "important" that their ISP offer Parental Controls
  - Parental Control is an important service that enables customers to manage their children's Internet activity and online safety." (Fil Giulione, VP Consumer ISP Marketing, Bell Canada)

- The vast majority of broadband households do not have the online protection they desire
  - 97% of households with kids don't use Parental Controls

III. Customer Perspective

- Purchasing: Parental Controls software will be available to download for FREE by all BIS customers.
- Downloading: .Net to host the FREE Parental Controls software download on the Portal. Customers may log-on to the Portal to download the software.
- Installing: Existing BIS customers may follow simple instructions for installing and set-up. Customers may log-on to the Portal to configure, set-up or revise the Parental Control profiles of family members.
- Customer Care: .Net will provide job aid and training for Help Desk ..... and will also provide Tier 2 customer support. They will answer any questions customer has about BIS Parental Controls.
- Billing: N/A

b) Alternate BellSouth Parental Control product

- BellSouth has launched a 2-Wire CPE based Parental Control product that is included with FastAccess HomeNetworking service. Additionally, FastAccess DSL customers who are not FastAccess HomeNetworking customers can opt to purchase the 2-Wire Parental Control / Firewall monitor solution at a cost of $6.95 per month plus the cost of the CPE.
  - The main benefits of the 2-Wire Parental Control product:
    - CPE-based protection in one convenient control box – no software to load.
    - Protection for any computer, game box, Internet/Web radio, video viewer etc that are part of the home network (regardless of OS or browser each computer uses)
  - Side-By-Side product comparison:
    - 2-Wire: CPE based ; BIS: software based.
    - 2-Wire: profiles are machine-specific ; BIS: profiles can be used on multiple computers
    - 2-Wire: Less inclusive customer reporting functionality
    - Filtering options appear to be equal (features, time online, time of day, content, etc)
    - Security features appear to be comparable

Section 2. Product Technology

2.1 What are BellSouth Parental Controls?

BellSouth Parental Controls were developed to help parents protect their children while surfing on the Internet. This easy-to-use interface will enable parents to set up different levels of access to websites for each child in their family. A parent will create a Master Account that will have control over what their children look at on the Internet as well as to set up how much time their children are allowed to access the Internet. Parents will be able to view each child's history of where they have been looking simply by running a usage report on each child. You can customize BellSouth Parental Controls to include child-specific settings for Web pages, chat rooms, objectionable word filtering, online time limits, and more!

2.2 Why should I have Parental Controls?

BellSouth Parental Controls help protect your children from the following types of sites:

Abortion

An abortion site is a site which provides information or arguments in favor of or against abortion; describes abortion procedures; offers help in obtaining or avoiding abortion; provides testimonials on the physical, social, mental, moral, or emotional effects, or the lack thereof, of abortion.

Alcohol

An alcohol site is a site which promotes or offers for sale alcoholic beverages or the means to create them; supplies recipes or paraphernalia; glorifies, touts, or otherwise encourages alcohol consumption or intoxication.

Drugs

A drug site is a site which promotes, offers, sells, supplies, encourages or otherwise advocates the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.

Gambling Categories

A gambling web site is a site where a user can place a bet or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing a bet; recieve instructions, assistance or training on participating in games of chance.

Hate Categories

A site which advocates hostility or aggression toward an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characterics; a site which denigrates others on the basis of those characteristics or justifies inequality on the basis of those characteristics; a site which purports to use scientific or other commonly accredited methods to justify said aggression, hostility or denigration.

Mature Content

Mature sexual content sites contain sexually explicit information that is not of a medical or scientific nature.

Porn Categories

A pornographic web site is a site containing sexually explicit material for the purpose of arousing a sexual or prurient interest.

Sex Education

A sex education site is a site which provides information on reproduction and sexual development, sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual orientation.

Tobacco

A tobacco content site is a site which encourages, promotes, offers for sale or otherwise encourages the consumption of tobacco.

Violence

A violence site is an anti-social web site which advocates or provides instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence.

Weapons

Guns

Guns pages are pages which offer for sale light or small arms, provide information on their procurement, describe or detail the function, performance or specifications of a given firearm or family of firearms.

Firearms Accessories

Firearms accessories pages offer for sale additional items for use in concordance with a gun, including attachments, modifiers, associated equipment or supplies, as well as repairs, refinishing, or other changes or alterations to the weapon or its component parts.

Knives
Knives pages offer for sale, advise how to procure, or advise how to make knives.

Martial Arts weapons pages are pages that sell, or advise on how to procure or manufacture, throwing or impact weapons designed for use in hand-to-hand fighting.

2.3 How does it work?

The definitions below will help you to understand how the Parental Controls software works and introduces you to the terms you should understand before setting up a Master Account and sub-accounts for your children.

Blocking	Not allowing a web browser to display the content of a web page
Categories	A grouping of various types of web pages.
Domains	The names or IP addresses of web sites such as www.domain.com or 209.247.228.201. (You can use the "www" or not.)
Domain (Allowing)	You have the ability to specify domains that you want to specifically **allow.**
Domain (Blocking)	You have the ability to specify domains that you want to specifically **block.**
Master Account	The main, or administrative, account your created when you subscribed to the BellSouth Portal (www.home.bellsouth.net) .
Sub-Account	Accounts you set up under the Master Account for other users of your BellSouth Dial-Up or DSL Service

2.4 System Preferences

Below are the system preferences that a customer may have to be able to run BellSouth Parental Controls.

Operating System Platforms	Windows XP Windows Me Windows 2000 *(SP 3 recommended)* Windows 98 Windows NT 4.0 NO MAC SUPPORT at this time
Processor	Intel Pentium or equivalent
Browsers	Microsoft Internet Explorer 5.0+
Available Disk Space	25 MB *(135 MB recommended for optimal performance)*
Total System Memory (RAM)	32 MB *(64 MB recommended for optimal performance)*
Client Size	1 MB
Download Time	5 minute download on most dial-up connections, within seconds on DSL.
Other	You should preferably be a registered user of the BellSouth Portal located at www.home.bellsouth.net

Section 3 - Installing the Software

3.1 User Authentication

To use, download the software for Parental Controls

Preferably, you are a BellSouth Internet Service Customer (Dial or DSL) and a registered user of the BellSouth Portal. Parental controls may be programmed to block you from downloading the software client if you don't meet the above criteria. Below is a diagram that demonstrates how a user may be authenticated.

Figure 1. Download and Set-Up Flow

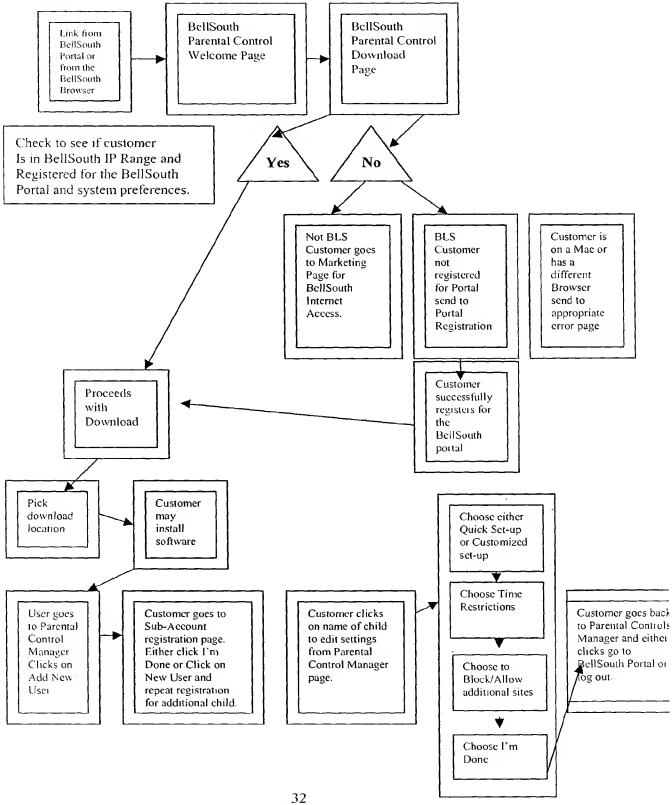
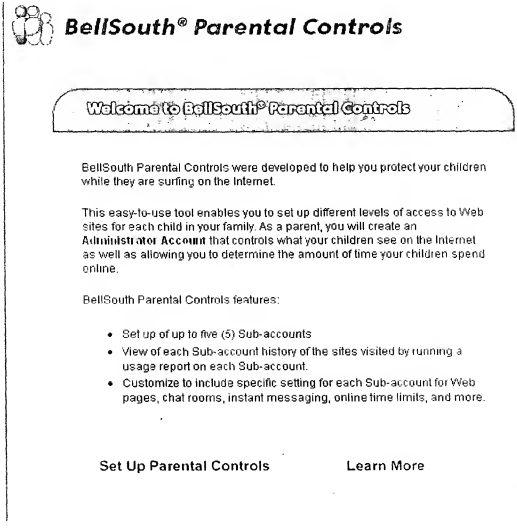
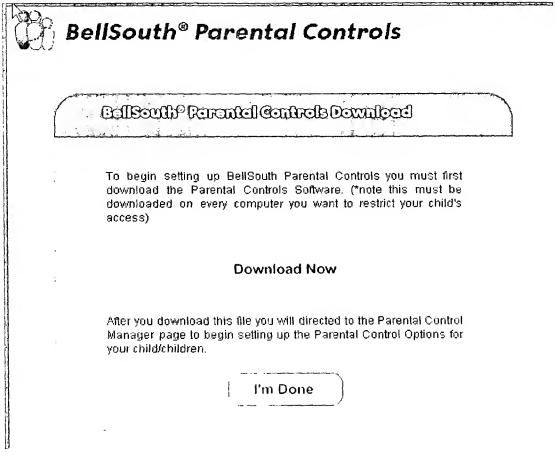


Figure 2. – Download Screens
Below this illustration demonstrates the process a customer will be directed through to set-up Parental Controls.

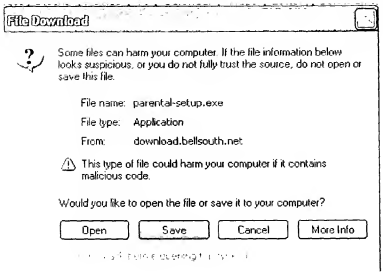
Step 1: BellSouth Parental Controls Welcome Page



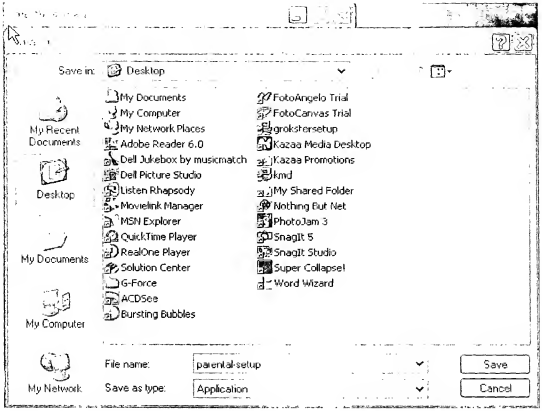
Step 2:
Parental Controls Download Page



Step 3: Download Software
Screen 1:

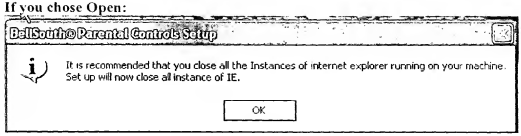


Screen 2: If you chose Save

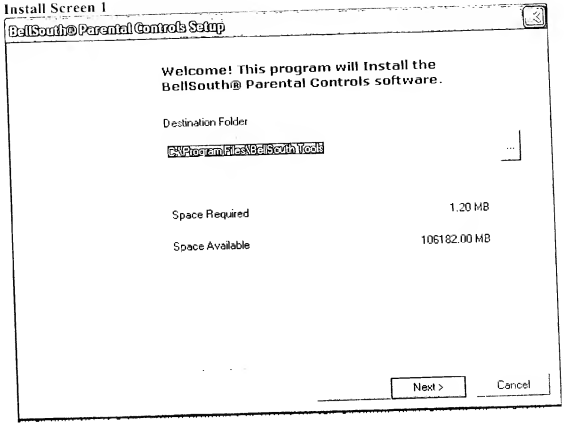


You would then have to go to where you saved it and double click on the icon to install the software and be directed to the Install Screens.

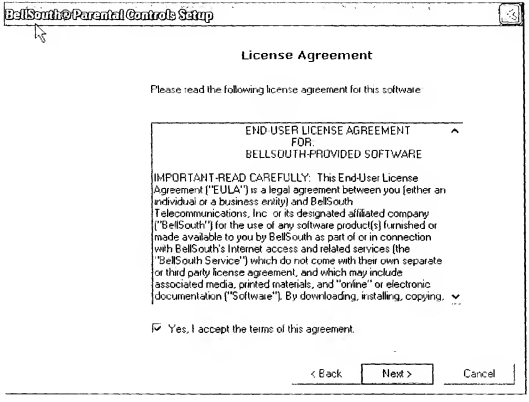
If you chose Open:



Install Screen 1



Install Screen 2



Install Screen 3

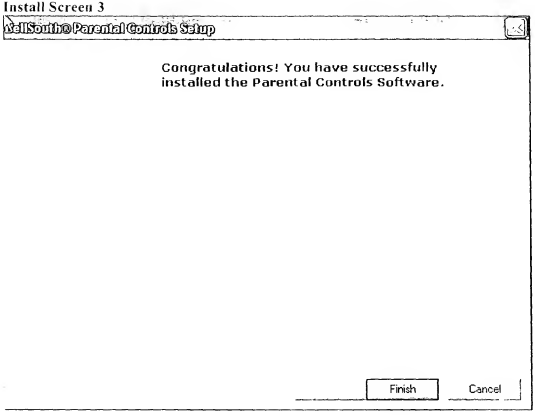
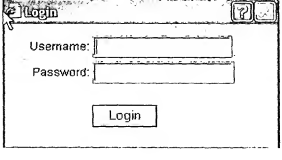


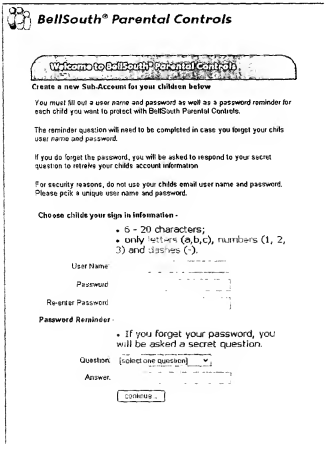
Figure 3 -Set-Up of Parental Controls

Login Screen:
Step 1: Login

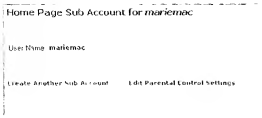


Step 2:
Parental Controls Manager

Step 3:
Add New User
Fill out user name, password and secret question for each child.



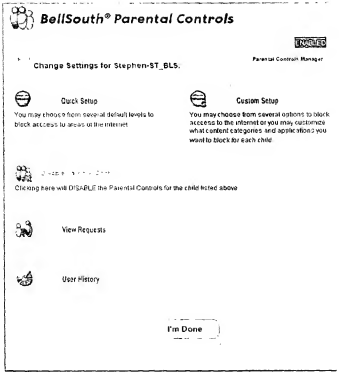
When all Sub Accounts are created click on Edit Parental Control Settings



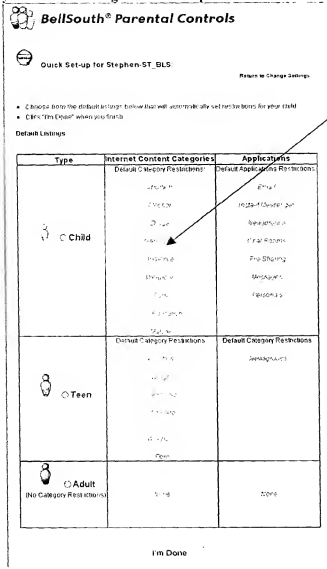
Step 4 – Parental Controls Set-up

Click on the child's name that you want to configure restrictions.
(Add Screen shot of Parental Controls Manager)

From the Settings page pick the type of set-up you want. You can either choose from Quick Set-Up or Custom Set-Up

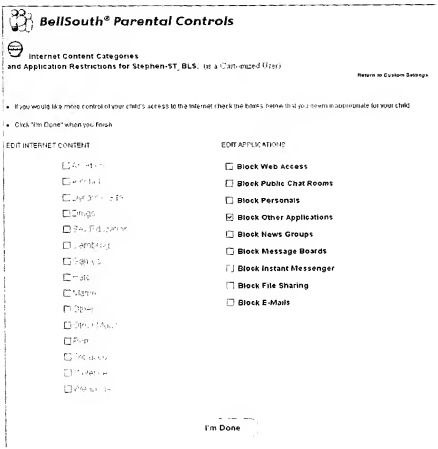


Quick Set-up Screen
The quick set-up defines the categories and application listed automatically to offer your child the highest level of protection.



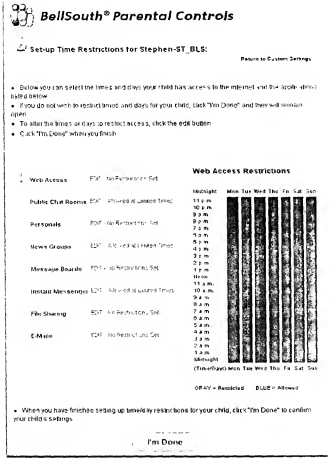
Choose the level you want to set for your child below. When finished click "I'm Done" if you change your mind click on "Return to Change Settings" button.

If you choose Custom Set-Up
You may pick (click in the boxes) from the categories and applications list below to customize a child's access. When finished click "I'm Done".

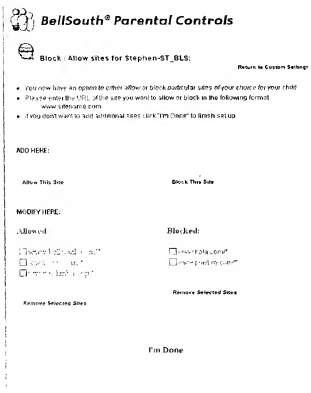


Set-Up Time Restrictions

You are now able to set time restrictions for Web Access and Applications. You can restrict particular times and days that you don't want your child to access the Internet. Simply click on the Edit button and you will go to a time setting for each application you want to edit.

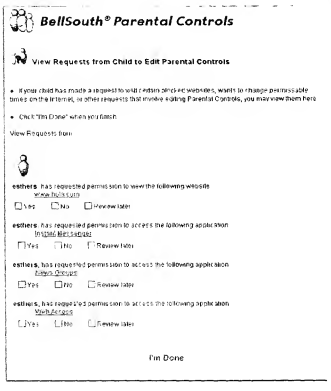


Block or Allow Sites
On this page you can alter the restrictions for your child to either block or allow particular sites.

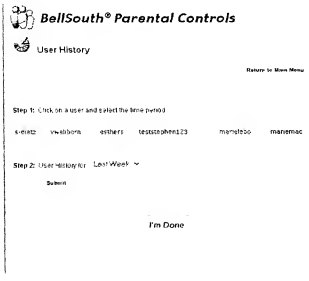


View Requests

When sites are blocked by BellSouth Parental Controls that your children think they should have access to, they can simply send a request to you asking for permission to view a site. You will be able to click on the site name and preview it first before you decide if you want to approve access to this site. A child can also ask for permission to get more time online.



Finally, from the Settings page you will be able to view your child's Internet History to find out exactly what they are doing online and how long they have been online for the previous day, week or month.



Section 4 – Error & Blocked Site Pages

Section 5 - System Tray Controls

You can access your Parental Control Manager from the Microsoft System Tray at the bottom right of your computer. Just look for the Parental Controls icon pictured below.

You then will use your mouse and right click on the icon. It will bring up a control menu where you can logout, block other software or click to got to the Parental Controls Manager where you have access to all of the controls to edit settings, add new users and get reporting.

Section 6- Parental Controls Frequently Asked Questions

1. What is BellSouth Parental Controls and how will it protect my children online?
2. What are the system preferences for BellSouth Parental Controls?
3. Why do I have to be registered for the BellSouth Portal to download Parental Controls?
4. How do I download Parental Controls?
5. How do I set-up accounts for my children?
6. What is the difference between quick set-up and customized set-up?
7. How do I sign into Parental Controls?
8. Why should I log-out after I am finished with an Internet session?
9. How can I edit restrictions for each child?
10. Where can I easily access the controls to manage Parental Controls from the system tray?
11. Do I have to be logged into the computer that I have downloaded Parental Controls on to modify my child's settings and can I manage them when I travel?
12. How to I approve/reject requests from my child to view sites or ask for more time on the Internet?
13. How do I view my child's user history so I can see what they have been doing online?
14. Can I have Parental Controls on more than one PC? If so, how do I configure it?
15. How is this different from the Parental Controls solution that is a part of BellSouth Home Networking?
16. Who do I contact if Parental Controls does not appear to be working correctly?
17. Can I use Parental Controls on a laptop?
18. Will Parental Controls work on a Mac Operating System?
19. Is Parental Controls offered in Spanish?

What is BellSouth Parental Controls and how will it protect my children online?
BellSouth Parental Controls was designed to help parents set up restrictions for children on how they access the Internet. Parental Controls will block inappropriate web content based on categories that BellSouth has defined unacceptable. Parents can also customize a child's access to block particular web applications such as Instant Messengers and Email clients and can also restrict the overall time their children are allowed to be online.

What are the system preferences for BellSouth Parental Controls?

Operating System Platforms	Windows XP Windows Me Windows 2000 *(SP 3 recommended)* Windows 98 Windows NT 4.0 NO MAC SUPPORT at this time
Processor	Intel Pentium or equivalent
Browsers	Microsoft Internet Explorer 5.0+
Available Disk Space	25 MB *(135 MB recommended for optimal performance)*
Total System Memory (RAM)	32 MB *(64 MB recommended for optimal performance)*
Client Size	1 MB
Download Time	5 minute download on most dial-up connections, within seconds on DSL.

Why do I have to be registered for the BellSouth Portal (www home.bellsouth.net) to download Parental Controls?
BellSouth Parental Control users should be registered for the BellSouth Portal to use Parental Controls. If you are not registered you will not be able to download the software necessary to enable Parental Controls to function. All of the functionality of this software is tied back to your BellSouth Portal account, including child's username and password, secret question and whatever restrictions you have set for a child. To register for the BellSouth Portal click here.

How do I download Parental Controls?
After you have successfully registered for the BellSouth Portal you will be able to access a screen where you can download the software. If you are not registered you will be directed to a registration page. You will click on the "Download Now" button to begin the installation process. You will be asked to either open the software from its current location or to pick a location on your computer where you want the software to be downloaded. After downloading the file you should install it. Please go to the area you downloaded the file and double-click on it to begin the installation process or if you clicked open from current location to begin the set-up process.

How do I begin setting-up accounts for each of my children?
Once you have successfully installed Parental Controls to your computer you can begin setting up sub-accounts for each of your children. To begin this process you should click on Add New User (show button) from the Main Parental Controls screen. You will be directed to a page (add screen shot of sub-account registration) where you should set-up specific user names and passwords for each child. This is the same information a child will use when they are prompted to login to Parental Controls each time they access the Internet. You can either set-up different user names and passwords for each child or use the same username and password, which will keep the same restriction levels for all of your children. When you have finished, please click on the button to return to Main page (insert a screen shot of this page) to return to begin setting up restriction levels.

What is the difference between quick set-up and customized set-up?
Parents can choose the Quick Set-Up, which will set-up default restrictions that are listed on the Quick Set-Up page that BellSouth has configured for a higher level of protection, or you can choose Customized set-up where a parent can customize what you want your children to do. In the Customized Set-up you may manually choose what restrictions you want to apply to your children.

Can I restrict the days and times my child accesses the Internet or specific applications?
Yes, BellSouth Parental Controls enables you to configure specific days and times that your child has access to the Internet. You can also block particular applications (i.e. Instant Messenger) from use by your children for particular times and days. You may go to the Edit settings screen to enable you to configure specific time restraints. (Insert Screen Shots here)

How do I sign into Parental Controls?
Once you have completely configured Parental Controls you will be asked to login each time you sign-on to the Internet. Parents will be asked for their login information and a child will be prompted to login as well. This is necessary to prevent children to be able to access the computer under their parent's username and password. (show screen shot of User Log-in screen).

Why should I to log-out after I am finished with an Internet session?
A parent should log-out of Parental Controls when they are signed in as the parent after finishing and Internet session. Once you log-out either the next time you boot up your computer or if you leave your computer on and your child tries to access it, they will be prompted to sign-in under their unique user name and password. If you forget to log-out after 30 minutes of inactivity BellSouth Parental Controls will automatically log you out.

How can I edit restrictions for each child?
After you set up custom restrictions for you children you can edit them from the Parental Controls Manager. Simply click on the name of the child you want to edit and you will be directed to a settings page. From here you will be able to set time restrictions, block/allow additional websites and block additional categories of Internet content and applications.

Where can I easily access the controls to manage Parental Controls from the system tray?
You can easily manage logging on and off and gain access to the Parental Control Manager by clicking on the icon in your Microsoft System Tray at the bottom right corner of your computer. You can also click on the tell-a-friend link to let other BellSouth Customers know that this feature is now available.

Do I have to be logged into the computer that I have downloaded Parental Controls on to modify my child's settings and can I manage them when I travel?

No, you don't have to be at the computer that you downloaded the software to manage your child's account. BellSouth's easy-to-use web interface enables you to view your child's history, accept or reject their requests and change settings on their accounts. You can do this from any PC with Internet Access, so you can do it from work or when you are traveling.

How to I approve/reject requests from my child to view sites or ask for more time on the Internet?

You can easily view requests for you child by clicking on the child's name from the Parental Controls Manager. You will be navigated to the settings page (insert screen shot) from here you can click on View Requests. In this area you will be able to either approve or reject requests from your children.

How do I view my child's user history so I can see what they have been doing online?

You will do exactly the same steps as you do to view requests, but instead of clicking on View Requests click on the User History link. You will navigate to a page that lists all of the sites that were visited and how many times visited by each child. You can also view how much time they spent on Applications such as Instant Messenger, email etc.

Can I have Parental Controls on more than one PC? If so, how do I configure it?
Yes, you can. You may sign into the BellSouth Portal with your username and ID. Then click on the Parental Controls link in the @BellSouth Module. You will be directed to the Parental Controls Manager. Click on the download for another computer. You will may install the software on that computer. You will not have to configure your settings for your children, because they will automatically appear on this machine when you login.

How is this different from the Parental Controls solution that is a part of BellSouth Home Networking Plus?
The BellSouth Home Networking Plus (link to BellSouth.com DSL Products) Parental Controls is pre-loaded on your BellSouth Gateway (mandatory equipment necessary to run Home Networking). You should be a Home Networking Plus subscriber to have access to this Parental Controls option. BellSouth Parental Controls will work with all BellSouth Internet Service (both Dial and DSL) Customers. No additional equipment is necessary to use BellSouth Parental Controls. You should subscribe to BellSouth Internet Service (either Dial or DSL) and that you are registered for the BellSouth Portal website (www.home.bellsouth.net).

Can I use Parental Controls on a laptop?
Yes, you can. You may have the BellSouth Parental Controls software downloaded and installed on your laptop and be signed in with your BellSouth Portal Account to activate Parental Controls.

Is Parental Controls offered in Spanish?
No, this product is not available in Spanish at this time, however it will block inappropriate website in Spanish.

APPENDIX 2

BellSouth Customized Browser (for integration with Pop-Up blocker and Parental Controls)

Purpose

The purpose of this project is to develop a visually pleasing easy to use Browser experience that is tied into the entire BellSouth Internet experience. It will have hooks into BellSouth Parental Controls, pop-up blocker, BellSouth search and BellSouth portal content.

Deliverables/Action Items

- Microsoft IEAK should be used to create a customized version of Microsoft Internet Explorer 6.0 based on the specifications provided in this document.
- The IE 6.0 files should support the following operating platforms: Win98, Win 98 SE, Win98 UPG, Win 2000, WinNT 4.0, Win ME, Win XP Home, Win XP Professional.
- The browser should be QA certified to work with the BellSouth portal site. In addition to a wide variety of other sites common to the Internet.

Graphic Files

They should be inserted as directed by the IEAK to appear during installation of the browser. Customized buttons should be designed to reflect the content they are representing.

Setup Wizard Left Bitmap with 256 colors (162 x 312 pixels)

Top Horizontal Bitmap with 256 colors (496 x 56 pixels)

Installation Options

The following components should be selected for installation:

Component	Download Version
Internet Explorer 6.0	Yes
Offline Browsing Pack	Yes
Internet Explorer Help	No
Default Media Player detection	Yes
Outlook Express	Yes
NetMeeting	No
Internet Explorer Browser Enhancements	Yes

Functionality
The BellSouth Browser will contain graphical representations of the most popular things to do online, such as search check email etc.

The buttons should occur in this order

1. Back – takes the customer back to the previous page
2. Forward – takes the customer forward a page.
3. Stop – Stops the page from loading
4. Refresh – refreshes the current page.
5. Home – Take the customer to their homepage (preset with www.home.bellsouth.net for default).
6. Search- will go to BellSouth Search
7. Tools – Will be a new button that will enable access to Parental Controls and Pop-up Catcher.
8. Favorites will include all of the Customers Favorites – as well as a folder full of all of the BellSouth Channels.
9. Video (will include links to the video vaults)
10. History – will show a customers history of sites visited.
11. Mail – will have hooks into BellSouth webmail and outlook.
12. Customize – this button with have options to customize your browser with additional buttons like radio, edit, Yellow pages etc.

Channel Button URLs in favorites

The favorites should appear as preinstalled bookmarks titled and ordered as indicated below. A customized BellSouth graphic should accompany each favorite in the Favorite pane.

BellSouth Customer Support:	home.bellsouth.net/csbellsouth
BellSouth Auto:	home.bellsouth.net/auto
BellSouth Auctions:	home.bellsouth.net/auctions
BellSouth Careers:	home.bellsouth.net/careers
Bellsouth Chat & People:	home.bellsouth.net/chatpeople
BellSouth Computers:	home.bellsouth.net/computers
BellSouth Entertainment:	home.bellsouth.net/entertainment
BellSouth Family:	home.bellsouth.net/family
BellSouth Games:	home.bellsouth.net/games
BellSouth Health:	home.bellsouth.net/health
BellSouth Money:	home.bellsouth.net/money
BellSouth News:	home.bellsouth.net/news
BellSouth Real Estate:	home.bellsouth.net/realestate
BellSouth Shopping:	home.bellsouth.net/shopping

BellSouth Small Biz:	home.bellsouth.net/atwork
BellSouth Sports:	home.bellsouth.net/sports
BellSouth Tax Center:	home.bellsouth.net/taxcenter
BellSouth Travel:	home.bellsouth.net/travel
BellSouth Video Vault	home.bellsouth.net/videovault

Pop up Catcher

Operating Systems Guidelines

Product is supported by Windows Operating Systems including Win 95, 98, 98SE, ME, NT, 2000 or XP.

Pop up Features

Basic Pop-Up and Pop-under control
Allow pop ups based upon site or application such as Internet Radio, Weather etc, new browser instances.
Logging of Pop up statistics
Distinctive Sound when Ad is blocked
Integrated with Internet explorer (toolbar or BellSouth browser)

Browser Support

Internet Explorer 5.x – 6.x
Netscape 4.x – 7.x

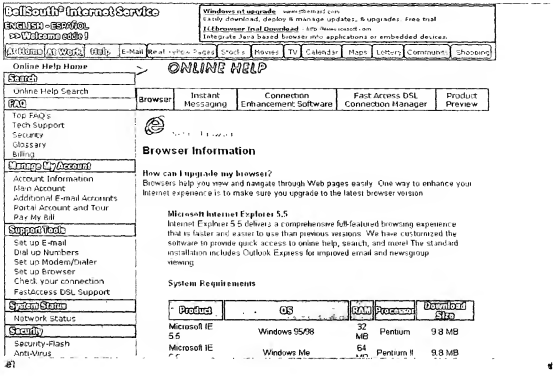
Tools Option

From the browser Tools Menu, the option to "Enable Pop-Up blocker" should be displayed. Selecting or unselecting it will enable or disable the pop-up management tool.

Sound Option

The sound option should be defaulted ON to present audio notification of a "caught" pop-up message.

Add the BellSouth Browser, Parental Controls and Pop-Up Blocker to the Online Help & Download Center link



Titlebar: BellSouth® Browser
Subtitle: BellSouth Browser with Pop-Up Catcher, Parental Controsl and Internet Explorer 6.0 SP1
Text: BellSouth Internet Services' customized browser with advanced features like the Pop-Up Catcher that allow you to avoid annoying pop-up ads while you surf and Parental Controls to help protect your children online. The BellSouth Browser is built on top of Microsoft's Internet Explorer and allows you the opportunity to upgrade to the latest IE 6.0 SP1 during the installation process.

For more information, system preferences or to download the BellSouth Browser, click here.

The "click here" should link the new browser information page detailed next. The existing "Browser Section" functionality should not change. The new link should go to a new page dedicated to information on the new BellSouth Browser.

Browser Information Page

The BellSouth Browser information page should have its own page with content solely dedicated to the browser. The new page should reflect the following verbiage:

BellSouth® Browser Information

BellSouth Internet Services' customized browser offers advanced features that help maximize your Internet browsing experience.

Pop-Up Catcher—allows you to avoid annoying pop-up ads while you surf.

Parental Controls – protect your children while they surf and block them from applications such as email, instant messenger and newsgroups.

Convenient Links—new icons and favorites allows you to access your most useful links like BellSouth portal content, e-mail and BellSouth Messenger right from the browser.

Internet Explorer 6.0—The BellSouth Browser is built on top of Microsoft's Internet Explorer and allows you the opportunity to upgrade to the latest IE 6.0 SP1 during the installation process.

System Preferences:

Operating System	Windows 98 SE + Windows Me Windows 2000 Windows XP (Home and Professional)
RAM	64 MB +
Processor	Pentium II +
Download Size	BellSouth Browser: 867 KB BellSouth Browser and IE 6.0: 12 MB
Download Time	Varies depending on connection type. Typical download time of the BellSouth Browser, without upgrading to IE 6.0, using a 28.8 kbps modem should take less than 5 minutes. Selecting the IE 6.0 upgrade may add over an hour to the download time.

To upgrade your browser, click on the Download Browser button below. A dialogue box will then appear: choose the "Run this program from its current location" option and click OK to begin the installation process.

DOWNLOAD BROWSER

Quick Trouble Shooting Guide

How can I disable my BellSouth Browser after it is installed?

1. Click on the computer's Start button.
2. Go to Programs
3. Select BellSouth, then BellSouth Browser
4. Select Enable-Disable BellSouth Browser
5. Click either Enable or Disable as desired.

Close all open browser sessions for the change to take affect. NOTE: Disabling the BellSouth Browser automatically disables the Pop-Up Catcher and Parental Controls as well.

How can I disable the Pop-Up Catcher?

1. Click on the browser's Tool menu.
2. Click on "Disable Pop-Up Catcher"

Disabling the Pop-Up Catcher will allow pop-ups to show normally on your screen.

How can I view a pop-up ad when Pop-Up Catcher is enabled?

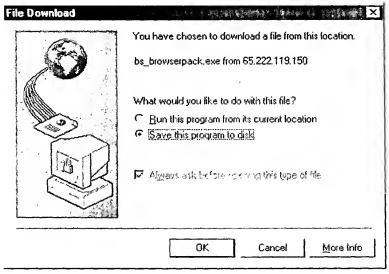
The Pop-Up Catcher actually "catches" the pop-up ad and puts a red "e" icon in the bottom status tray of the browser. If your sound is enabled, the program will also audio alert. To view the ad, click on the red "e" icon and it will open the page.

What if I don't like the icons that were added to my Tool Bar?

Internet Explorer allows you customize which icons appear and the order in which they appear.

1. Position your mouse over a blank area of the Tool Bar and right-click.
2. Click "customize" and follow the instructions given to manipulate the icons.

After clicking "Download Browser" on the page above, customers should be sent directly to the Microsoft installation dialogue box to begin the browser installation process. The dialogue box is copied below as reference. The box is provided and controlled by Microsoft, so BellSouth has no control over its contents.

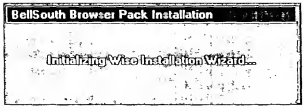


Assumptions

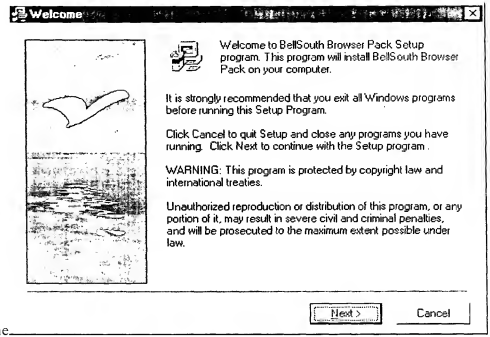
- Default screen size is 800 by 600 pixels

Install Screens

BP01-Initializing

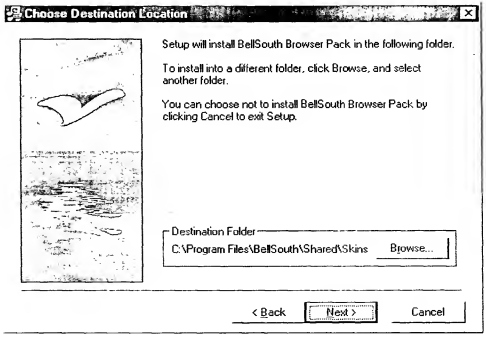


BP02-

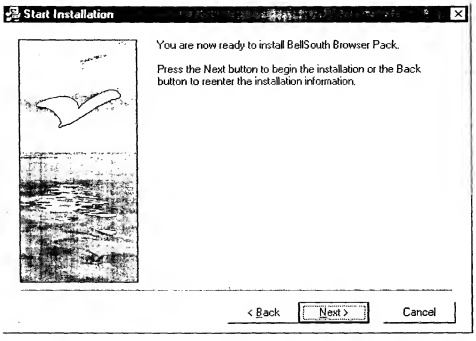


Welcome

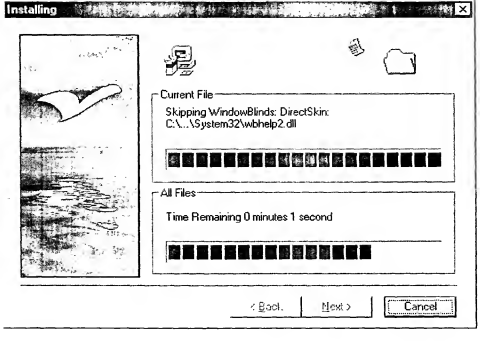
BP03-Destination Folder



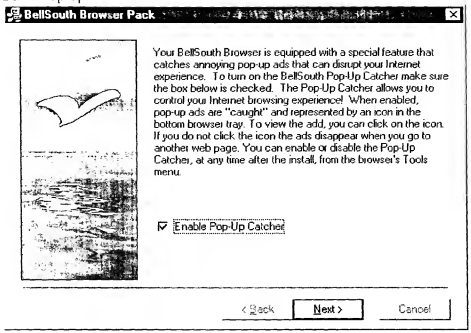
BP04-Start



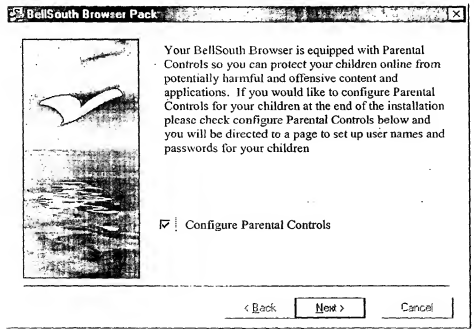
BP05-Installing

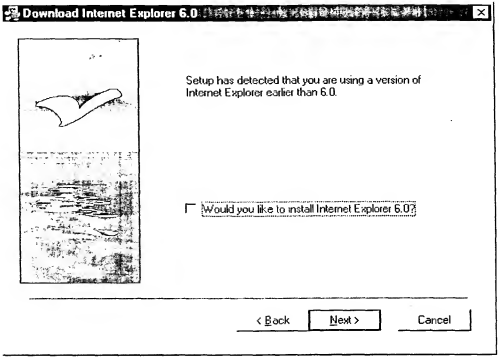


BP07-Pop-up

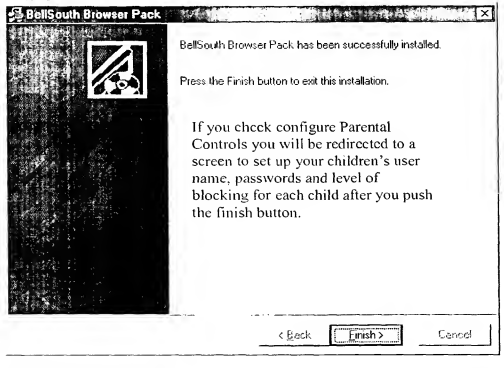


BP08-IE6



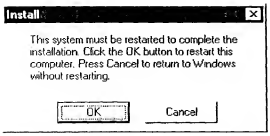


BP09-Success

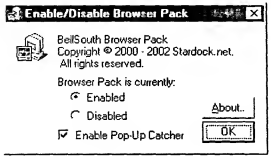


If they enable Parental Controls they will be redirected to the Parental Controls download set up after they click on the Finish screen. If they don't want Parental Controls the download is over. (See Parental Control document for set-up instructions.

BP10-Restart



Enable/Disable Box



Tools Button

The tools button on the BellSouth Browser should include the following:

Enable/Disable Pop-up Catcher
Enable/Disable Sound with Pop-up Catcher
Parental Controls Edit/Set-up
Help with Parental Controls
Help with Pop-up Blocker

Parental Controls/Pop-Up Blocker will not be available to customers who do not use our browser. It should be a part of it to make accessing the enable/disable and help screens easy to access by our customers.

APPENDIX 3

BellSouth Parental Control- Basic Concepts

1. Categorize Web and Software

Web Categories:

All Internet web sites are divided into the following categories. General categorization data-feed is provided from RuleSpace. Additional categories such as email sites, chat sites, message-board sites are defined by BellSouth.

Abortion, Drugs, Gambling, Porn, Violence, Search, Public Chat Rooms, Message Boards, E-Mails.

Software Categories:

Software applications are divided into the following categories completely defined by BellSouth

Browsers (Netscape, IE, Opera, MSN, AOL), E-Mails (outlook), Instant Messengers, News Groups (outlook express), File Sharing (Kaaza, Napster).

2. Allow, Disallow or Time Restrict Categories

Categories can be either completely allowed, disallowed, or time restricted (such as between 8:00 am to 10 pm).

Different timings can be set for a particular day , weekend, weekdays, and everyday.

3. User Overrides

Parents have ability to override or black-list any web sites.

Parents have ability to black-list any software applications from their PCs.

4. Master and Sub Accounts

There is a master (or parent) account that can have up to 5 sub-accounts for their children. The parent only has access to setup and change the children's Parental Control Settings.

Parental Control Settings are tied to the individual accounts rather than the specific machines they are using, so that machines can be shared.

5. Components of Software

Client Component:

This is a part of the Parental Control software that users may download and install on individual PCs. No user specific settings are stored in this software ; in some embodiments.

Remote Admin:

This is a web site (part of BellSouth portal) where parents can go edit any settings for sub-accounts. This is accessible from any machine having Internet access

Synchronization:

The Client Component forces users to login if the user is not already logged in. It then pulls all the latest changes from Remote Admin for the current user.

Synchronization also happens at the very first instance of a browser or on restarting the machine.

6. User Activity Reports

Parents are provided with a daily, weekly, monthly reports of their children's activities. Reports include for each child: websites visited, category of website, number of visits, software used, category of software, time spent

7. Request For More Permissions

Children can request the parents for permissions to have access to the restricted categories, can ask for more time, and allow access to specific websites

Parents can view and approve/disapprove requests from the Remote Admin site

3. Identifying Software

EXE name,
Company Name
Product Name

Main Window Title
Main Window Class
Main Window Style

ABSTRACT OF THE DISCLOSURE

[0070] The present disclosure provides systems and methods for controlling access to computing services. Some embodiments provide access control mechanisms for controlling access to computer applications and services based on settings within a user's configuration profile. The configuration profile of user of a general-purpose computer is specified by the primary user of the general-purpose computer. In this manner, the primary user of the general-purpose computer may control and regulate the type of access that others users of the general-purpose computer have to local computer applications and other computer services.

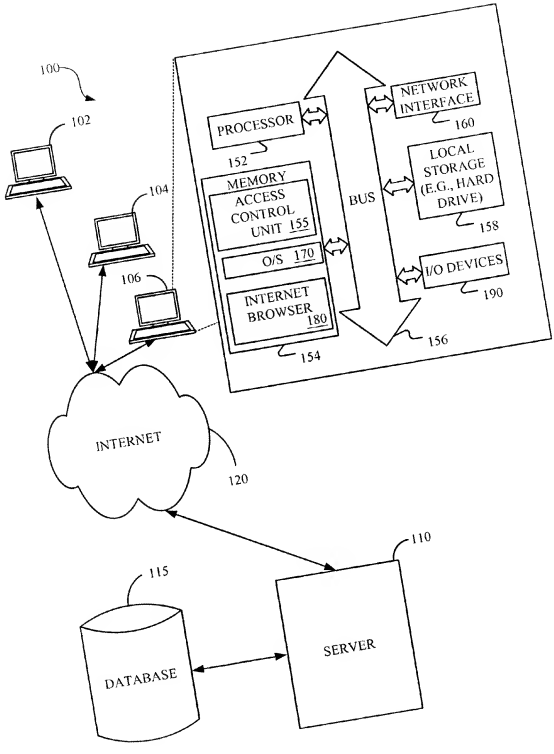

100
102
104
106
PROCESSOR
152
MEMORY
ACCESS
CONTROL
UNIT 155
O/S 170
INTERNET
BROWSER
180
154
BUS
156
NETWORK
INTERFACE
160
LOCAL
STORAGE
(E.G., HARD
DRIVE)
158
I/O DEVICES
190
INTERNET
120
110
115
DATABASE
SERVER

FIG. 1

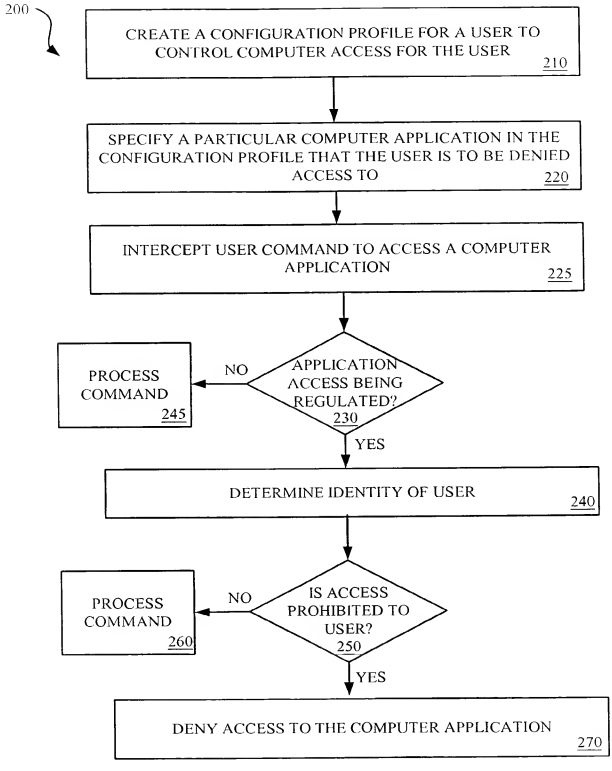

200
CREATE A CONFIGURATION PROFILE FOR A USER TO CONTROL COMPUTER ACCESS FOR THE USER
210
SPECIFY A PARTICULAR COMPUTER APPLICATION IN THE CONFIGURATION PROFILE THAT THE USER IS TO BE DENIED ACCESS TO
220
INTERCEPT USER COMMAND TO ACCESS A COMPUTER APPLICATION
225
APPLICATION ACCESS BEING REGULATED?
230
NO
PROCESS COMMAND
245
YES
DETERMINE IDENTITY OF USER
240
IS ACCESS PROHIBITED TO USER?
250
NO
PROCESS COMMAND
260
YES
DENY ACCESS TO THE COMPUTER APPLICATION
270

FIG. 2

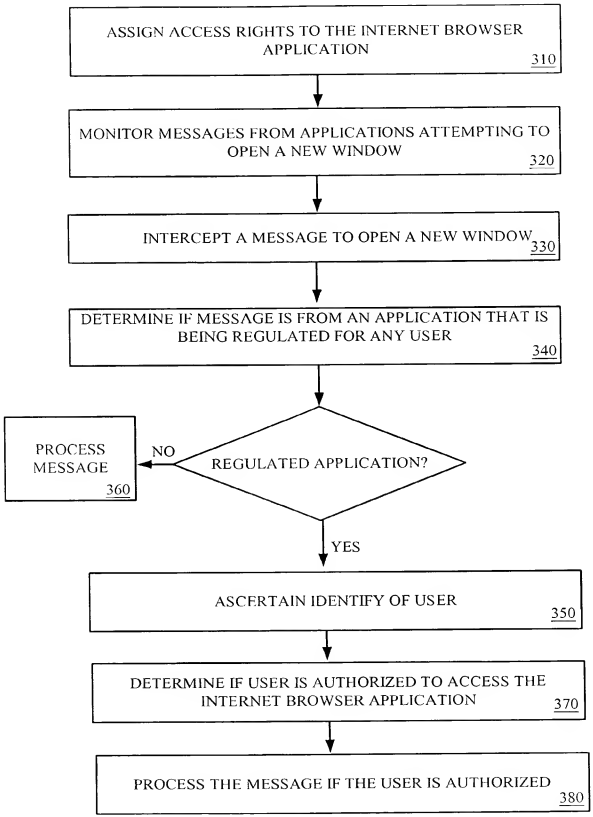

ASSIGN ACCESS RIGHTS TO THE INTERNET BROWSER APPLICATION
310
MONITOR MESSAGES FROM APPLICATIONS ATTEMPTING TO OPEN A NEW WINDOW
320
INTERCEPT A MESSAGE TO OPEN A NEW WINDOW
330
DETERMINE IF MESSAGE IS FROM AN APPLICATION THAT IS BEING REGULATED FOR ANY USER
340
REGULATED APPLICATION?
NO
PROCESS MESSAGE
360
YES
ASCERTAIN IDENTIFY OF USER
350
DETERMINE IF USER IS AUTHORIZED TO ACCESS THE INTERNET BROWSER APPLICATION
370
PROCESS THE MESSAGE IF THE USER IS AUTHORIZED
380

FIG. 3

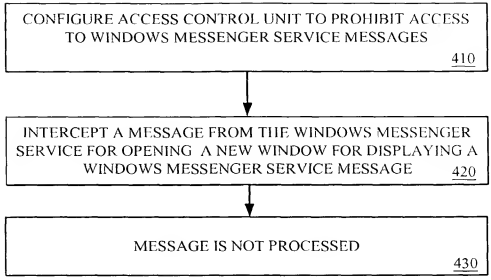

CONFIGURE ACCESS CONTROL UNIT TO PROHIBIT ACCESS TO WINDOWS MESSENGER SERVICE MESSAGES
410
INTERCEPT A MESSAGE FROM THE WINDOWS MESSENGER SERVICE FOR OPENING A NEW WINDOW FOR DISPLAYING A WINDOWS MESSENGER SERVICE MESSAGE
420
MESSAGE IS NOT PROCESSED
430

FIG. 4

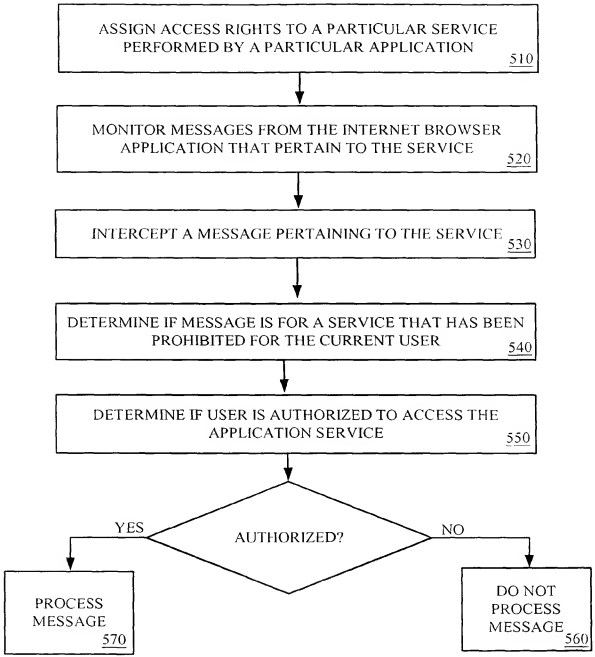

ASSIGN ACCESS RIGHTS TO A PARTICULAR SERVICE PERFORMED BY A PARTICULAR APPLICATION
510
MONITOR MESSAGES FROM THE INTERNET BROWSER APPLICATION THAT PERTAIN TO THE SERVICE
520
INTERCEPT A MESSAGE PERTAINING TO THE SERVICE
530
DETERMINE IF MESSAGE IS FOR A SERVICE THAT HAS BEEN PROHIBITED FOR THE CURRENT USER
540
DETERMINE IF USER IS AUTHORIZED TO ACCESS THE APPLICATION SERVICE
550
AUTHORIZED?
YES
NO
PROCESS MESSAGE
570
DO NOT PROCESS MESSAGE
560

FIG. 5

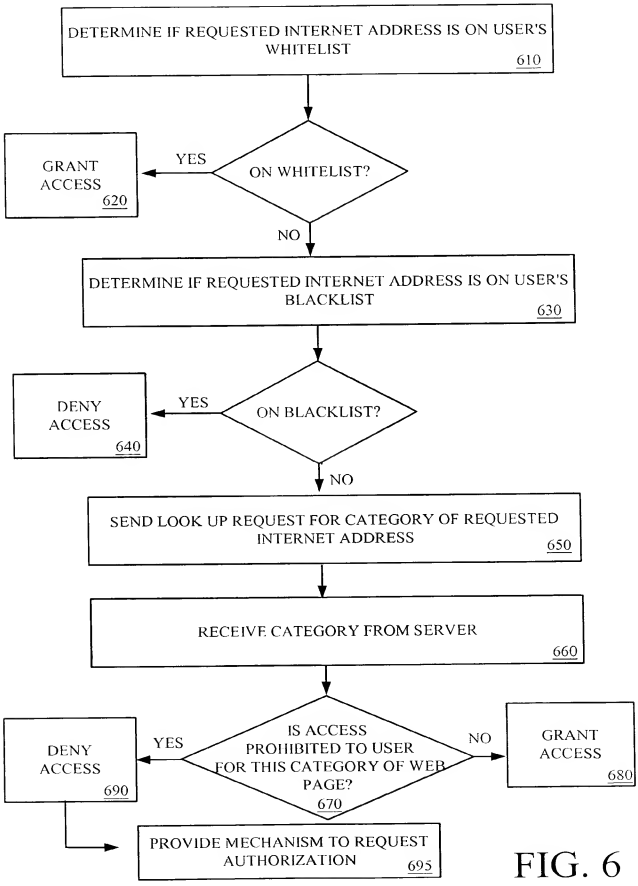

DETERMINE IF REQUESTED INTERNET ADDRESS IS ON USER'S WHITELIST
610
ON WHITELIST?
YES
GRANT ACCESS
620
NO
DETERMINE IF REQUESTED INTERNET ADDRESS IS ON USER'S BLACKLIST
630
ON BLACKLIST?
YES
DENY ACCESS
640
NO
SEND LOOK UP REQUEST FOR CATEGORY OF REQUESTED INTERNET ADDRESS
650
RECEIVE CATEGORY FROM SERVER
660
IS ACCESS PROHIBITED TO USER FOR THIS CATEGORY OF WEB PAGE?
670
YES
DENY ACCESS
690
NO
GRANT ACCESS
680
PROVIDE MECHANISM TO REQUEST AUTHORIZATION
695

FIG. 6

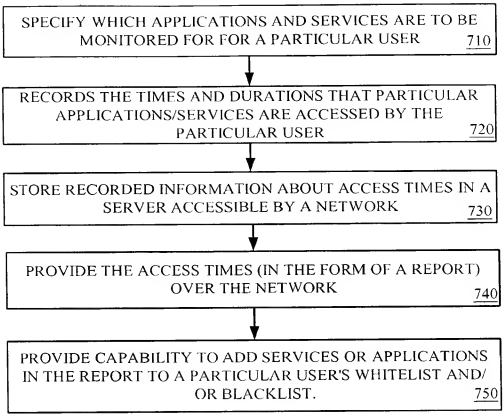

SPECIFY WHICH APPLICATIONS AND SERVICES ARE TO BE MONITORED FOR FOR A PARTICULAR USER 710
RECORDS THE TIMES AND DURATIONS THAT PARTICULAR APPLICATIONS/SERVICES ARE ACCESSED BY THE PARTICULAR USER 720
STORE RECORDED INFORMATION ABOUT ACCESS TIMES IN A SERVER ACCESSIBLE BY A NETWORK 730
PROVIDE THE ACCESS TIMES (IN THE FORM OF A REPORT) OVER THE NETWORK 740
PROVIDE CAPABILITY TO ADD SERVICES OR APPLICATIONS IN THE REPORT TO A PARTICULAR USER'S WHITELIST AND/ OR BLACKLIST. 750

FIG. 7

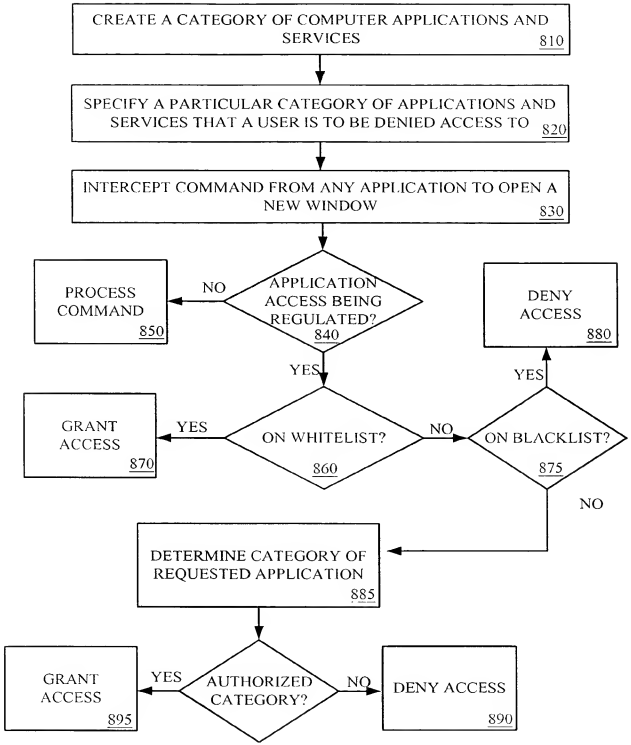

CREATE A CATEGORY OF COMPUTER APPLICATIONS AND SERVICES
810
SPECIFY A PARTICULAR CATEGORY OF APPLICATIONS AND SERVICES THAT A USER IS TO BE DENIED ACCESS TO
820
INTERCEPT COMMAND FROM ANY APPLICATION TO OPEN A NEW WINDOW
830
APPLICATION ACCESS BEING REGULATED?
840
NO
PROCESS COMMAND
850
YES
ON WHITELIST?
860
YES
GRANT ACCESS
870
NO
ON BLACKLIST?
875
YES
DENY ACCESS
880
NO
DETERMINE CATEGORY OF REQUESTED APPLICATION
885
AUTHORIZED CATEGORY?
YES
GRANT ACCESS
895
NO
DENY ACCESS
890

FIG. 8

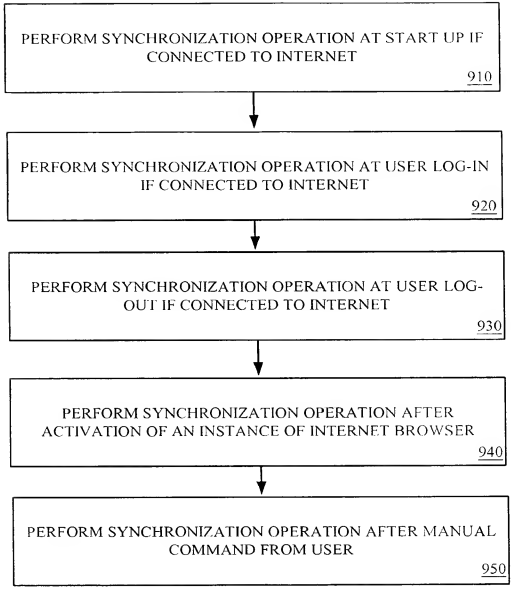

PERFORM SYNCHRONIZATION OPERATION AT START UP IF CONNECTED TO INTERNET
910
PERFORM SYNCHRONIZATION OPERATION AT USER LOG-IN IF CONNECTED TO INTERNET
920
PERFORM SYNCHRONIZATION OPERATION AT USER LOG-OUT IF CONNECTED TO INTERNET
930
PERFORM SYNCHRONIZATION OPERATION AFTER ACTIVATION OF AN INSTANCE OF INTERNET BROWSER
940
PERFORM SYNCHRONIZATION OPERATION AFTER MANUAL COMMAND FROM USER
950

FIG. 9